Command Line Interface (CLI) for Cisco Unified Communications Domain Manager 8.1.3

First Published: October 31, 2013
Last Modified: October 31, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Command Line Interface (CLI) for Cisco Unified Communications Domain Manager 8.1.3

Contents

Overview

This document is a guide to assist administrators and system engineers understand the CUCDM Server command line interface.

Note

The content of this document covers highly technical tasks that can have serious consequences if not implemented correctly. It has been created for advanced administrators and system engineers.

This system supports various deployments/solutions including HCS and Large Enterprise (LE). This document describes the product in general and is not specific to a particular deployment/ solution. Information may vary slightly depending on the installation environment.

Typographic Conventions

The following typographic conventions are used in this document:

Item	Character format	Example
Buttons	**Bold**	Click the **Enter** button.
Checkboxes	*italic*	Select the *Country* checkbox.
Dialog boxes menu items, tab names, radio buttons	*italic*	Select the *Configuration* option, or select the *Parameters* tab.

CHAPTER 1

Introduction

The command line interface (hereafter CLI) replaces the functionality that was provided by webmin in previous server installations. The CLI is used to perform system maintenance.

CHAPTER 2

Functionality

The following tasks can be carried out via the CLI:

- Upgrade the system software
- Reboot or shutdown the system
- Backup and restore the database
- Change the network settings
- View log files
- Enable, disable and check debugging status
- Query system status and health summary
- Stop and start all services
- Monitor services
- Restore failed services
- Test network connectivity
- Upgrade the software
- Check the Disaster Recovery (DR) status
- Put DR nodes into standby or active mode
- Synchronize DR standby nodes

CHAPTER 3

Usage

Logging into the CLI

To use the CLI, a client capable of SSH is required. The most common SSH clients include Putty (Windows platform) or the SSH client in a terminal (UNIX / Linux or Mac OS X platform).

Note

The password for the USMCLI user is specified when installing the system. Please contact the engineer that installed the system in order to query the password. The default password is 'usmcli'.

Procedure

To use the CLI:

Step 1 SSH to CUCDM and login as the user *usmcli*. A command prompt is displayed (see typical example below):

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>>

=>>
```

From here you are able to perform the following functions:

- help
- enable
- health
- history
- ping
- exit

Step 2 After entering each menu, a list of available commands is displayed.

Some commands (displayed in square braces, e.g. enable) are actually submenus. To change into the submenu, simply enter the command name. The prompt will change to indicate which menu you are currently in. To return to the previous menu, use *exit*.

TAB auto-completion can be used - enter the first few characters of the command name and press TAB. Many commands also have support for TAB completion to display the available options.

Help is also available for the following:

- Display the current menu options using *help*
- Display help on a particular command by entering *help command*
- Display the menu structure using *help menu*
- Display the menu structure with all sub-commands using *help menu full*

Step 3 To enter the enable menu (similar to other networking hardware) type enable as shown below:

```
=>>enable
=>#
```

The prompt should change from "=>>" to "=>#" to reflect this change.

Once in the Enable menu, the following functions are available:

- [autoregister]
- [backup]
- [configuration]
- [destinations]
- [dhcp]
- [dr]
- [logging]
- [network]
- [snmp]
- [software]
- [system]
- [webservices]
- health
- history
- exit

Each of these commands and menus are described in the Available Commands section below.

Configurable options

Many of the submenus have configurable options pertaining to that menu function. The show command displays the available options that can be configured, together with the current value. The output of the show command is displayed when you enter a submenu.

Use the set command to change the value of an option. Tab completion can be used to complete the option name on the command line

Usage: set option value

To save the values permanently and apply the changes to the running system, use the apply command. You will be prompted if you wish to continue, if you answer yes to the prompt you will be requested to enter your name. This is used to keep a record of changes that were made to the system. If an attempt is made to exit the menu before applying changes, the system will query whether you wish to exit without applying the changes.

Note

Applying changes restarts services and should only be performed within maintenance windows.

CHAPTER 4

Available Commands

Health

The health report displays a summary of the system status with the following sections

- Versioning displays the version numbers for the platform and application
- Provisioning shows information about the different elements that are provisioned in the internal database
- System status displays the system resource usage
- Network status shows the network interfaces
- Disk status shows the mounted file volumes and the disk usage

- Service status shows each of the functional business services and whether that service is experiencing problems
- Shared filesystem and DR periodic sync shows the last few synchronisation events between Primary and Standby hosts
- Backup and Restore duration indicate when backups were made or restored
- System summary is a high-level overview of warnings which require action on the part of the administrator

When the administrator logs into the CLI front-end, the system looks for warnings that may be present. If warnings are detected, the CLI will notify the administrator of these when entering a new menu. Many of these warnings serve to notify the administrator of issues that would affect production systems, such as incorrect hardware configuration, lack of backup scheduling, etc. In a test environment, the administrator may choose to ignore some of these warnings.

Health report output

```
Current time: 2012-07-13 10:25:47.016659
Uptime: 1 day, 19:08, 1 user, load average: 0.11, 0.13, 0.09

Versioning:
-----------
Platform version: 4.3.092-0.4.275
     USM version: usm-8.0.999+svn69082

Provisioning:
-------------
    1 providers
    1 resellers
    6 customers
   12 locations
    0 subscribers
  387 phones
  381 phones
  387 devices

System status:
--------------
     AVAIL  CPUs=2   Memory=7876 MB

Network status:
---------------
eth0      Link encap:Ethernet  HWaddr 00:0c:29:8c:7a:a4
          inet addr:10.120.1.3  Bcast:10.120.1.255  Mask:255.255.255.0
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0

Disk status:
------------
                              / has  71% free space (  15G avail of   21G)
               /srv/VOSS/shared has  92% free space ( 4.6G avail of  5.0G)
                /srv/VOSS/pgsql has  90% free space ( 160G avail of  178G)
                  /srv/VOSS/dhcp has  92% free space ( 924M avail of 1008M)
             /srv/VOSS/estraier has  92% free space ( 4.6G avail of  5.0G)
                  /srv/VOSS/imq has  93% free space ( 3.7G avail of  4.0G)

Service status:
---------------
   Disaster Recovery : OK
            Selfcare : OK
         BulkLoaders : OK
    AutoRegistration : OK
            AdminGUI : OK
           Telephony : OK

Shared filesystem hourly sync:
------------------------------
```

```
2012-07-13T06:17:02 - Shared filesystem hourly sync of 1s with size 13312KB
and throughput 13312.0KB/s

DR periodic sync:
-----------------
2012-07-13T10:25:01 - DR periodic sync of 1s with size 16384KB and throughput 16384.0KB/s

Backup duration:
----------------
2012-07-10T16:48:00 - Backup duration of 5s with size 414KB and throughput 73.2KB/s

Restore duration:
-----------------
2012-07-10T17:04:12 - Restore duration of 173s with size 414KB and throughput 2.4KB/s

System summary:
---------------
! Minimum CPU requirement is 7 or more
! Minimum memory requirement is 32Gb
```

Note that DR sync, filesystem sync, and automated backups are only performed on hosts in Primary mode, and cannot be performed on a host while in DR Standby mode. On DR Standby nodes it is normal for the aforementioned services to remain inactive.

Ping

The ping command is used to test network connectivity to a remote host

Ping output

```
=>> ping cpt-pxe-01
Pinging cpt-pxe-01
5 packets transmitted, 5 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.345/0.638/1.563/0.464 msen
```

Enable

This is used to enter privileged configuration mode.

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable
enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=>#
```

Once in the Enable menu, the following functions are available:

- [autoregister] is used to manage the phone autoregistery service
- [backup] is used to manage system backups
- [configuration] can be used to view and export the configuration file
- [destinations] define endpoints where backups, reports, snmp traps, etc. can be delivered to

- [dhcp] is used to manage the DHCP service
- [dr] is used to configure and manage the Disaster Recovery capability
- [logging] is used to configure the debugging levels within the system
- [network] defines the network parameters
- [snmp] configures the SNMP service, including SNMP queries and traps
- [software] is used to upgrade the system software
- [system] can be used to manage the routine maintenance of system services
- [webservices] is used to manage the webservices function
- health displays a health status report
- history displays a history of previous commands executed
- exit to exit

DR

This is used to manage Disaster Recovery.

Note

For more information, please refer to the *Redundancy and Disaster Recovery Guide* document.

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=>#  dr

Documented commands (type "help menu | <topic>"):
================================================
exchange_keys     history           make_primary      make_standby      setup
state             sync              exit

=>[dr] #
```

- exchange_keys

  This command is used to exchange authentication keys between Primary and Standby hosts for Disaster Recovery synchronisation. Normally this is performed automatically by the system.

- State

  This displays the synchronisation state between the Primary and Standby nodes, showing whether synchronisation is up to date, etc.

- Sync

Sync the current Standby node to the Primary. Use this command if the two systems do not sync, or have lost sync at some point - this will take approximately ten minutes, depending on data size.

- Exchange keys

  Exchange security keys between DR nodes. This is automatically performed by CUCDM, but can be performed manually if DR is failing to synchronize.

- Make primary

  Puts this standby node into Primary/Active state - this takes approximately ten minutes.

  Best practices for a DR system

  - Make sure DR is setup correctly
  - Make sure that the Primary and Secondary servers do not have the same IP
  - Make sure that a health check via the CLI is performed at least once per week, Identify warnings: in particular disk space, DR related problems and backups
  - Make sure backups are performed (hourly, daily, weekly etc...)
  - Make sure that SNMP and mail alerts are setup
  - Make sure that a separate back volume is used
  - Test that all destinations added are working (use the test function in the CLI)
  - Make sure the time is correct and `ntp` is configured. Ensure snapshots are taken before upgrades. Make sure that your platform version is up to date. Make sure that your system complies with the minimum specifications: 32 Gigs Ram, 7 CPU's.

- Make standby

  Makes this node a standby - this takes approximately ten minutes, dependent on data size.

- Setup

  Used to setup DR on an Active/Primary server that did not have DR setup initially. It requires the IP of the standby server - this takes approximately ten minutes, dependent on data size.

DHCP

DHCP is used to manage the phone IP address assignment service

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=># dhcp

Documented commands (type "help menu | <topic>"):
```

```
================================================
apply       history     set         show        exit

List of configurable options (show, set):
-----------------------------------------
|OPTION  |VALUE |DESCRIPTION                   |
|------  |----- |-----------                   |
|Enabled |True  |Enable or disable DHCP Service |

=>[dhcp] #
```

The DHCP service can be enabled using the command *set enabled true* and disabled with *set enabled false*

Autoregister

This is used to configure the autoregistration of phones.

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=># autoregister

Documented commands (type "help menu | <topic>"):
================================================
apply       history     set         show        exit

List of configurable options (show, set):
-----------------------------------------
|OPTION         |VALUE |DESCRIPTION                  |
|------         |----- |-----------                  |
|Request_expiry |3600  |Autoregister retry timelimit |

=>[autoregister] #
```

The autoregister service has a timeout value (default 3600s) which can be adjusted in this menu.

Webservices

This will manage Web services

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit
```

```
=>#  webservices

Documented commands (type "help menu | <topic>"):
================================================
apply       history     set         show        exit

List of configurable options (show, set):
-----------------------------------------
|OPTION  |VALUE |DESCRIPTION                                          |
|------  |----- |-----------                                          |
|Enabled |False |Enable Webservice                                    |
|8.1.0   |True  |Enable version 8.1.0 webservices interface           |
|8.0.0   |False |Enable version 8.0.0 compatible webservices interface |

=>[webservices] #
```

Webservices can be enabled using the command *set enabled true*.

Different webservice interfaces can be deployed simultaneously to provide backward compatibility to 3rd party systems. Each version of the webservices interface that is available is listed under the available options - each interface can be enabled or disabled separately.

Network

Networking settings. This is used to alter the network parameters.

Note

When CUCDM is in standby mode, the administrator can only change the IP of its Primary server. All other settings are disabled until CUCDM is changed to Primary node.

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=>#  network

Documented commands (type "help menu | <topic>"):
================================================
[routes]       apply          history        nslookup       ping           set
show           traceroute     exit

List of configurable options (show, set):
-----------------------------------------
|OPTION     |VALUE                    |DESCRIPTION               |
|------     |-----                    |-----------               |
|Fqdn       |172.29.248.213           |FQDN Address              |
|Address    |172.29.248.213           |Systems IPv4 Address      |
|Nodename   |martin                   |Node name of system       |
|Domainname |visionoss.int            |Domain name of system     |
|Netmask    |255.255.255.0            |ipv4 netmask              |
|Gateway    |172.29.248.1             |Default gateway for system |
|Dns        |172.29.88.11,172.29.88.56 |DNS server list           |
|Ntp        |172.29.1.15              |NTP server list           |
```

```
=>[network] #
```

The following options can be configured using the *set* <*option*> <*value*> command:

- Fully qualified domain name (e.g. hostname.domainname)
- IP address of the host
- Hostname
- Domain name
- Network netmask
- Default gateway
- DNS server. A comma (,) separated list of DNS servers can be provided.
- NTP server

The NTP server is very important to the correct configuration and operation of the system. In particular, NTP provides an accurate time source to maintain the consistency of transaction timing, filesystem health, and the remote synchronisation of transactions in a DR (Disaster Recovery) system. It is highly preferable that both DR primary and standby nodes have an accurate NTP source.

Additionally, the nslookup, ping, and traceroute commands can be used to test network reachability

Static Routes

This manage network static routes.

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=># network

Documented commands (type "help menu | <topic>"):
================================================
[routes]       apply          history        nslookup       ping           set
show           traceroute     exit

List of configurable options (show, set):
-----------------------------------------
|OPTION     |VALUE                    |DESCRIPTION               |
|------     |-----                    |-----------               |
|Fqdn       |172.29.248.213           |FQDN Address              |
|Address    |172.29.248.213           |Systems IPv4 Address      |
|Nodename   |martin                   |Node name of system       |
|Domainname |visionoss.int            |Domain name of system     |
|Netmask    |255.255.255.0            |ipv4 netmask              |
|Gateway    |172.29.248.1             |Default gateway for system |
|Dns        |172.29.88.11,172.29.88.56 |DNS server list           |
|Ntp        |172.29.1.15              |NTP server list           |
```

```
=>[network] # routes

Documented commands (type "help menu | <topic>"):
================================================
add         apply       delete      history     show        exit

=>[network] [routes] #
```

- Show

  List current static routes.

- Add

  Add a static route

  Usage: add <destination>[/netmask] <gateway>.

- Del

  Delete a static route

  Usage *del <destination>[/netmask]*

- Apply

  Save and implement Static routes.

As an example, the administrator can add a route as follows:

```
 =>[network] [routes] # add 10.1.1.0/24 10.120.1.0
 =>[network] [routes] # show
 |OPTION      |VALUE      |DESCRIPTION                                        |
 |------      |-----      |-----------                                        |
 |10.1.1.0/24 |10.120.1.0 |Net 10.1.1.0 Mask 255.255.255.0 via 10.120.1.0  |
```

Destinations

The destinations submenu is a central point where destination endpoints can be defined. These named endpoints can be used by other functions to send files or reports to.

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=># destinations

Documented commands (type "help menu | <topic>"):
================================================
add         apply       delete      edit        history     set         show        test
exit

Current destinations:
---------------------
support_email : email to support@voss-solutions.com
```

```
snmp_trap_dest1 : snmp trap to None
snmp_trap_dest2 : snmp trap to None
files : sftp to vossadm@172.29.248.213:/tmp/ppp

=>[destinations] #
```

In this menu, `show` displays a list of named destinations. The administrator can perform a variety of actions of these destinations:

- `edit` can be used to modify the destinations configuration
- `test` will attempt to send a file to the destination in order to test that the destination's configuration is correct
- `delete` will delete the named destination

You can add a new destination by entering "add" and following the onscreen prompts.

```
=>[destinations] # add
Select a protocol used to send to the destination
 [  1 ]  local
 [  2 ]  email
 [  3 ]  sftp
 [  4 ]  scp
 [  5 ]  ftp
 [  6 ]  snmptrap

Select one of the above options; <ENTER> to quit... 2

These names are already used: snmp_trap_dest1,snmp_trap_dest2

Select a name for the new destination? support
List of configurable options (show, set):
----------------------------------------
|OPTION    |VALUE                      |DESCRIPTION             |
|------    |-----                      |-----------             |
|Relayhost |172.29.1.1                 |SMTP relay host         |
|From      |support@voss-solutions.com |From email address      |
|Addresses |                           |List of email addresses |

=>[destinations] [support] #

=>[destinations] [support] # help

Documented commands (type "help menu | <topic>"):
================================================
add         apply       delete      edit        history     set         show        test
exit
```

The first prompt asks for the type of destination

- `local` allows files to be stored on the local filesystem
- `email` sends a file to an email address
- `sftp` sends the file to a remote SFTP server
- `scp` sends the file to a remote SCP address
- `ftp` sends the file to a remote FTP server
- `snmptrap` defines a new SNMP trap destination.

The second prompt is for a name to reference the destination by

Once the destination is created, you will notice that the prompt has changed and your view is restricted to the configurable options of the destination.

You can now edit the options in the normal way, and once the configuration is completed, use "apply" to save the changes.

Note that in order to test the destination, you must apply the changes first.

Also note that a preceding / (slash) in the path will indicate an absolute path - many systems such as sftp require a relative path without a preceding /

For example, this following sequence would add a new email address:

```
=>[destinations] # add

Select a protocol used to send to the destination
 [  2 ]  email
Select one of the above options; <ENTER> to quit... 2

Select a name for the new destination? remotemail

List of configurable options (show, set):
----------------------------------------
|OPTION    |VALUE                     |DESCRIPTION             |
|------    |-----                     |-----------             |
|Relayhost |172.29.1.1                |SMTP relay host         |
|From      |support@voss-solutions.com |From email address      |
|Addresses |                          |List of email addresses |

=>[destinations] [remotemail] # set addresses support@voss-solutions.com
=>[destinations] [remotemail] # apply
```

The following example shows how to add a sftp destination (which could be used to remotely copy scheduled backups, as an example):

```
 =>[destinations] # add

 Select a protocol used to send to the destination
  [  3 ]  sftp
 Select one of the above options; <ENTER> to quit... 3

 Select a name for the new destination? remotesftp

 List of configurable options (show, set):
 ----------------------------------------
 |OPTION   |VALUE       |DESCRIPTION           |
 |------   |-----       |-----------           |
 |Username |            |Username              |
 |Path     |/           |Path on remote server |
 |Password |*****       |Password              |
 |Hostname |example.com |Server name           |
 |Port     |22          |Port                  |

 =>[destinations] [remotesftp] # set username sftp
 =>[destinations] [remotesftp] # set path backups
 =>[destinations] [remotesftp] # set password sftp123
 =>[destinations] [remotesftp] # set hostname 10.120.1.4
 =>[destinations] [remotesftp] # apply

 =>[destinations] # test remotesftp
 Sending of file/s was successful
```

The following example shows how to add a snmp trap destination (to which all snmp traps are automatically forwarded to):

```
=>[destinations] # add

Select a protocol used to send to the destination
 [  6 ]  snmptrap
Select one of the above options; <ENTER> to quit... 3
```

```
 Select a name for the new destination? nmsforsnmp

 List of configurable options (show, set):
  |OPTION    |VALUE       |DESCRIPTION                                                  |
  |------    |-----       |-----------                                                  |
  |Hostname  |example.com |Server name to send SNMP traps to                            |
  |Version   |2c          |SNMP version to use ; "apply" for version dependent fields |
  |Community |public      |SNMP v2c community string                                    |
  |Mode      |Trap        |Sent Trap or Inform message                                  |

 =>[destinations] [nmsforsnmp] # set hostname 10.120.1.4
 =>[destinations] [nmsforsnmp] # set version 2c
 =>[destinations] [nmsforsnmp] # set community public
 =>[destinations] [nmsforsnmp] # set mode trap
 =>[destinations] [nmsforsnmp] # apply

 =>[destinations] # test nmsforsnmp
 Trap sent successfully
  Please ensure that a trap was received at this destination
```

Configuration

View and export system configuration.

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=>#  configuration

Documented commands (type "help menu | <topic>"):
================================================
audit              config_history     history            send               view
exit

=>[configuration] #
```

In this menu you can perform the following actions on the system configuration file:

- `view` displays the configuration file to the screen
- `send` will send the configuration file to a remote system
- `audit` is used to verify whether the configuration file matches the physical configuration files deployed on the system
- `config_history` displays the history of changes made

Logging

This is used to manage and view system diagnostics logs.

```
Welcome to the CLI management console
```

```
Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]           [configuration]     [destinations]
[dhcp]              [dr]               [logging]           [network]
[snmp]              [software]         [system]            [webservices]
health              history            exit

=># logging

Documented commands (type "help menu | <topic>"):
================================================
[performance]        apply               history              list
send                 send_transaction    set                  show
view                 exit

List of configurable options (show, set):
-----------------------------------------
|OPTION               |VALUE |DESCRIPTION                                    |
|------               |----- |-----------                                    |
|Health_dest          |None  |Destination to copy health reports to          |
|Health_email         |None  |Destination to email health report to          |
|Apache_debug         |False |Set Apache debug logging True or False         |
|Nginx_debug          |False |Set Nginx debug logging True or False          |
|Iptcore_debug        |False |Set Iptcore debug logging True or False        |
|Ipttestfeature_debug |0     |Set Ipttestfeature debug level from 0 .. 4     |
|Platform             |True  |Set platform debug logging True or False       |
|Application          |False |Set application debug logging True or False    |
|Remote_syslog        |None  |Send syslog message to IP; disable with 0.0.0.0 |

=>[logging] #
```

Please note that debugging should only be used by support staff and impacts performance of the system. Do not enable debugging on production systems unless the system is being actively monitored.

All the debug options described above result in additional logging at the system level. The ipttestfeature allows for device logging to be enabled on the GUI front-end.

- list shows a list of available log files that can be viewed
- `view` displays a particular log file to the screen
- `send` transmits an archive of the logfiles to a named destination
- `send_transaction` destination> <transaction#> sends a trace of a specific transaction to the destination <transaction>

There are a number of configuration options that can be configured using "set", and "apply"

- `health_dest` is a destination to which daily health reports are sent to
- `health_email` is a destination to which daily health reports are emailed
- `remote_syslog` is an IP address to which syslog events should be sent

In addition, there are a number of debug flags that can be enabled to diagnose a system. Note that these debug flags will increase the amount of debugging performed by the system, and could affect the performance of the system.

In order to send logfiles, the "send" command will prompt with a list of destinations that it can use to send the logfiles. These destinations are created in the "Destinations" menu. The following example shows how a new email address is created, and the logfiles sent to that email address

```
=>> en
=># destinations
=>[destinations] # add

Select a protocol used to send to the destination
 [  2 ]  email
Select one of the above options; <ENTER> to quit... 2
Select a name for the new destination? remotemail

List of configurable options (show, set):
-----------------------------------------
|OPTION    |VALUE                      |DESCRIPTION             |
|------    |-----                      |-----------             |
|Relayhost |172.29.1.1                 |SMTP relay host         |
|From      |support@voss-solutions.com |From email address      |
|Addresses |                           |List of email addresses |

=>[destinations] [remotemail] # set addresses support@voss-solutions.com
=>[destinations] [remotemail] # apply
=>[destinations] # exit
=># logging

Documented commands (type "help menu | <topic>"):
================================================
[performance]        apply                history              list
send                 send_transaction     set                  show
view                 exit

=>[logging] # send

Destinations available:
 [  1 ]  remotemail - email to ['support@voss-solutions.com']
Select one of the above options; <ENTER> to quit... 1
<support@voss-solutions.com>
Sending of file/s was successful
```

Performance

This is used to retrieve and analyze system performance statistics

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=># logging

Documented commands (type "help menu | <topic>"):
================================================
[performance]        apply                history              list
send                 send_transaction     set                  show
view                 exit

List of configurable options (show, set):
-----------------------------------------
|OPTION               |VALUE |DESCRIPTION                                  |
|------               |----- |-----------                                  |
|Health_dest          |None  |Destination to copy health reports to        |
```

```
|Health_email         |None  |Destination to email health report to          |
|Apache_debug         |False |Set Apache debug logging True or False         |
|Nginx_debug          |False |Set Nginx debug logging True or False          |
|Iptcore_debug        |False |Set Iptcore debug logging True or False        |
|Ipttestfeature_debug |0     |Set Ipttestfeature debug level from 0 .. 4     |
|Platform             |True  |Set platform debug logging True or False       |
|Application          |False |Set application debug logging True or False    |
|Remote_syslog        |None  |Send syslog message to IP; disable with 0.0.0.0 |

=>[logging] # performance

Documented commands (type "help menu | <topic>"):
================================================
health          history         send            set             show            summary
transaction     exit

List of configurable options (show, set):
-----------------------------------------
|OPTION |VALUE               |DESCRIPTION                                      |
|------ |-----               |-----------                                      |
|Start  |2012-07-12 00:00:00 |Start of the period to analyze: yyyy-mm-dd HH:MM:SS |
|End    |2012-07-12 14:57:06 |End of the period to analyze: yyyy-mm-dd HH:MM:SS   |

=>[logging] [performance] #
```

The performance menu is used to analyze performance metrics in the system.

- `summary` shows a performance summary
- `transaction` is used to analyse a particular transaction id
- `send` is used to send performance reports to a named destination

The performance summary is analyzed between the 'start' and 'end' times. These times default each time from midnight to the current time of day. However, they can be adjusted using the `set` command.

Software

To query, upgrade and maintain software packages.

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=># software

Documented commands (type "help menu | <topic>"):
================================================
[scripts]         [vmware]          history           language_pack     packagelist
upgrade           exit

=>[software] #
```

Software can be upgraded using the "upgrade" command. Upgrade files must first be uploaded to the system using a SFTP or SCP client to usmcli@hostname. The 'upgrade' command will list the available upgrades, indicating whether the upgrade is for the system or application. You will

be prompted to confirm whether a VMware snapshot has been taken before the upgrade. This is imperative in order to revert the software upgrade afterward.

Please refer to the System Upgrade Guide.

Do not attempt to upgrade CUCDM when it is in standby mode. Please refer to the *Redundancy and Disaster Recovery Guide* when attempting to upgrade a DR server. This command takes approximately ten minutes to run.

VMware tools

Manage VMware tools installation. These tools are used for better integration into VMware

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=># software

Documented commands (type "help menu | <topic>"):
================================================
[scripts]         [vmware]          history           language_pack     packagelist
upgrade           exit

=>[software] # vmware

Documented commands (type "help menu | <topic>"):
================================================
history       install       status        uninstall     exit

=>[software] [vmware] #
```

VMware can be installed or uninstalled from this menu.

`status` displays whether the vmware tools are installed.

The system is shipped with the VMWare system client version 4.1. If this system is installed on VMWare 5 ESXi host, the VMware tools can be upgraded by mounting the VMware Tools CD from the ESXi host, and then reinstalling VMware tools using the `uninstall` and `install` commands from the vmware menu

Scripts

This will run scripts on CUCDM.

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
```

```
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=>#  software

Documented commands (type "help menu | <topic>"):
================================================
[scripts]         [vmware]          history           language_pack     packagelist
upgrade           exit

=>[software] # scripts

Documented commands (type "help menu | <topic>"):
================================================
history      list         password     run          exit

=>[software] [scripts] #
```

This menu provides functionality to run external scripts to supplement the functions already provided by the CLI. These scripts are encrypted and digitally signed to ensure that they do not pose a risk to the system. Scripts must first me uploaded to the system via a SFTP client to the following directory sftp@hostname:scripts/

Note that the scripts must be placed in the scripts directory or they will not be located.

`run` can be used to display a list of available scripts, and execute a script once selected.

The default password for the SFTP user is "sftp", but can be changed using the `password` function.

System

To manage system services.

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=>#  system

Documented commands (type "help menu | <topic>"):
================================================
cleanup          cleardown        diskadd          diskshow         history
monitor          password         reboot           reinitialize     shutdown
startall         stopall          time             tune             exit

=>[system] #
```

The following functions can be used to manage the system:

- `shutdown` halts the server, and attempts to power off the server automatically
- `reboot` performs a system reboot

- `password` is used to change the "usmcli" password
- `monitor` is used to monitor the state of services, while "monitor all" will continuously display service state until Ctrl-C is pressed.
- `cleanup` attempts to clear any existing services that are in a failed state - this is normally continuously managed by the system.
- `reinitialise` is a more aggressive command co assist with service problems and initialise the system correctly
- `stopall` is used to stop all services and takes approximately five minutes to complete.
- `startall` is used to start all services again and takes approximately five minutes to complete.
- `cleardown` is a highly destructive procedure that destroys all data in the database. Do not use this command unless you fully understand the consequences. The command takes approximately 15 minutes to complete.
- `tune` is used to retune the system when additional hardware (e.g. CPU and/or memory) has been added to the system
- `time` allows VMware time synchronisation to be enabled only when NTP service is not currently configured.
- `diskshow` displays the disk structure that is in use by the system
- `diskadd` is used to add a new system or backup disk to the system.

In order to add a new disk to the system, the disk is first provisioned via Vsphere and assigned to the VM. The `diskadd` command will then detect the new disk, and you can indicate the purpose of the additional storage

The system may be deployed originally without a backup disk. This is not an optimal setup, and a backup disk can be added after the fact to ensure that backups are stored seperate and cannot be deleted during a "cleardown" operation. Typically the backup disk should be at least 100Gb in size, or about five times the size of the database to provide sufficient space for multiple backups.

A system disk can be added so that additional services, e.g. DHCP, WebServices, AutoRegister, can be enabled after initial install.

The `diskadd` can also be used to increase the size of the swap partition. This may be necessary for crash dump reporting, i.e. a crashdump file is generated in the event of a kernel panic. In order to generate a crashdump, the swap partition needs to be sufficiently large to store a dump of all memory usage, and the crashdump image is stored in /var/crashdump only if sufficient space is available on the disk.

Time synchronisation is very important to the correct configuration and operation of the system. In particular, NTP (configured in the Networking menu) provides an accurate time source to maintain the consistency of transaction timing, filesystem health, and the remote synchronisation of transactions in a DR (Disaster Recovery) system. It is highly preferable that both DR primary and standby nodes have an accurate NTP source, rather than relying on VMware time synchronization

The tune command is used to reconfigure the system if any hardware changes have been made. These changes include changes to memory and/or CPUs. It is also used if the MAC address of the ethernet adapter has been changed (common if the VM is cloned) - this is diagnosed by the absence of eth0 and presence of eth1 in the health report, as well as indicates in the syslog. By running 'tune', all services are stopped, the system reconfigured, and the system restarted again.

Backup

To perform backup, restore and manage scheduled backups.

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=># backup

Documented commands (type "help menu | <topic>"):
================================================
apply       backup      delete      history     list        restore     set         show
exit

List of configurable options (show, set):
-----------------------------------------
|OPTION         |VALUE        |DESCRIPTION
|------         |-----        |-----------
|Enabled        |True         |Enable automated backup system
|Number         |5            |Number of backups to keep
|Retention_days |7            |Number of days to keep backups
|Remote_dest    |martin       |Destination to copy backup files
|Email          |martin_email |Destination to email reports to
|Sched_time     |00:00        |At what time of the day should the backup be run
|Sched_days     |*            |Which days of the week should backups run.
                                Comma seperated list. Sunday = 0 |

=>[backup] #
```

- `backup` will manually perform a system backup, either to the database or backup volume
- `restore` is used to restore the database from a backup file
- `delete` is used to delete an existing backup file

Automatic backups can be made by configuring the options. Automatic backups are enabled using the `enabled` option. The number of backups that are kept can be adjusted using `retention_days` and `number`.

`sched_time` and `sched_days` are used to schedule when backups are performed.

Normally backups are stored on the local host, but these can be copied off-host by configuring the `remote_dest` destination.

`email` is used for backup delivery reports

For more information, please read the *Backup and Restore* document.

SNMP

To manage SNMP configuration options

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health       history      ping         exit

=>> enable
```

```
Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=>#  snmp

Documented commands (type "help menu | <topic>"):
================================================
[trap]      apply       history     set         show        exit

List of configurable options (show, set):
-----------------------------------------
|OPTION       |VALUE  |DESCRIPTION                                      |
|------       |-----  |-----------                                      |
|Enabled      |True   |Enable or disable SNMP Queries                   |
|Community    |public |SNMP v2c Community String                        |
|Username     |None   |SNMP v3 Username                                 |
|Password     |*****  |SNMP v3 Password                                 |
|Query_source |None   |SNMP query_source                                |
|Sysname      |None   |Name of this server                              |
|Syslocation  |None   |Location of this server                          |
|Syscontact   |None   |Contact person(s) for this server (email address)|
|Load1        |4      |1 Minute load average alarm value                |
|Load5        |3      |5 Minute load average alarm value                |
|Load15       |2      |15 Minute load average alarm value               |

=>[snmp] #
```

Set

The following options can be set with the set command.

- Enabled -Enable or disable SNMP Queries
- Community- SNMP v2c Community String used to query this server
- Username - SNMP v3 Username to query this server
- Password - SNMP v3 Password to query this server
- Query_source - IP address that is allowed to query this server
- Sysname - Name of this server, as it will appear when queried via SNMP
- Syslocation - Location of this server
- Syscontact - Contact person(s) for this server (email address)
- Load1 - one minute load average alarm value
- Load5 - five minute load average alarm value
- Load15 - 15 minute load average alarm value

Trap

To manage SNMP trap destinations. CUCDM can be configured to send SNMP to a number of different trap destinations.

```
Welcome to the CLI management console

Documented commands (type "help menu | <topic>"):
================================================
[enable]     health      history      ping        exit
```

```
=>> enable

Documented commands (type "help menu | <topic>"):
================================================
[autoregister]      [backup]            [configuration]     [destinations]
[dhcp]              [dr]                [logging]           [network]
[snmp]              [software]          [system]            [webservices]
health              history             exit

=># snmp

Documented commands (type "help menu | <topic>"):
================================================
[trap]      apply       history     set         show        exit

=>[snmp] # trap

Documented commands (type "help menu | <topic>"):
================================================
add         apply       delete      edit        history     set         show        test
exit

Current destinations:
---------------------
admin_email : email to admin@host.com
snmp_trap_dest1 : snmp trap to  123.45.6.7
snmp_trap_dest2 : snmp trap to None
admin : sftp to admin@123.45.6.7:/tmp/ppp

=>[destinations] #
```

You will note that the prompt has changed to `destinations`. This is because SNMP traps simply produce traps to all valid destinations of type `snmp_trap` type.

By deleting or adding destinations of type `snmp_trap`, the system is configured to use these for SNMP traps.

Please refer to the section describing the Destinations menu for further information

CHAPTER 5

Appendix

Classless Inter-Domain Routing (CIDR)

Classless Inter-Domain Routing (CIDR) notation is a specification of an Internet Protocol address and its associated routing prefix. CIDR notation is constructed from the IP address and the prefix size, the latter being the number of leading *1* bits of the routing prefix. The IP address is expressed according to the standards of IPv4 or IPv6. It is followed by a separator character, the forward slash (/) character, and the prefix size expressed as a decimal number.

The address may denote a single, distinct, interface address or the beginning address of an entire network. In the latter case, the CIDR notation specifies the address block allocation of the network. The maximum size of the network is given by the number of addresses that are possible with the remaining, least-significant bits below the prefix. This is often called the host identifier.

For example:

- The address specification `192.168.100.1/24` represents the given IPv4 address and its associated routing prefix `192.168.100.0`, or equivalently, its subnet mask `255.255.255.0`.
- The IPv4 block `192.168.0.0/22` represents the 1024 IPv4 addresses from `192.168.0.0` to `192.168.3.255`.

Fully Qualified Domain Name (FQDN)

- Fully qualified domain name (FQDN) is the absolute domain name of a host - it is usually the hostname appended by the domain name. It is expected that the FQDN will be resolvable by DNS queries.
- Example: server1.example.com
- If a host does not have a FQDN, the host's IP address can be used.